REMARKS

Claims 1-3 and 5-16 were rejected in the above-identified Final Office Action and remain pending. Claims 4 and 17-19 were previously cancelled. No claims are currently amended, added, or cancelled in this response.

Reconsideration of the rejections is respectfully requested in light of the remarks below.

CLAIM REJECTIONS UNDER 35 U.S.C. § 103

In "Claim Rejections – 35 USC § 103," item 3 on page 2 of the above-identified FOA, claims 1-3 and 5-16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2002/0156921 to *Dutta et al.* (hereinafter Dutta) in view of U.S. Patent No. 6,865,655 to *Andersen* (hereinafter Andersen) and further in view of U.S. Patent No. 6,526,316 to *Ramasubramani et al.* (hereinafter Ramasubramani).

Applicants respectfully traverse the rejections.

Section § 103 requires both the invention being examined and the references to be viewed "as a whole."

Claim 1 recites, in part, "a memory comprising computer executable instructions . . . operative to cause the wireless communication apparatus to:

> facilitate login, by a user of the wireless communication apparatus, to a user account at a remote backup server, the user account being accessible from the wireless communication apparatus as well as from another computing device of the user;
>
> facilitate designation, by the user, of data on the wireless communication apparatus to be backed up by the backup server;
>
> generate a hash value for said designated data;
>
> communicate a request to the backup server to back up the designated data, including said hash value, to enable said backup server to determine whether said data is already available to said backup server;

only after said backup server determines that said data was not already earlier made available to said backup server from the wireless communication device or other devices, receive a request from said backup server to send said data to said backup server; and

send said data to said backup server in response to said request from the backup server, wherein the backup server is configured to store the data, to associate the stored data with said user account as well as other user accounts subsequently wanting to backup the same data, and to provide, on request by the user, the data to the another computing device of the user."

Accordingly, viewed properly as a whole, claimed 1 is directed to a wireless communication apparatus with executable instructions for a backup method that requires (1) login by a user to a user account at a remote backup server, and (2) user selection of data to be backed up. The user account at the remote backup server must also be accessible from another computing device of the user. The remote backup server must be configured to provide the data to that other computing device on request by the user. Moreoever, the backup server must be further configured to store the data and to associate the stored data with the user account *as well as with other user accounts*.

Additionally, the *backup server* must determine – in response to a backup request *from the wireless communication device* – whether the data designated by the user for backup is already available to the backup server. *If the data is unavailable to the backup server*, the backup server must send a request for the data to the wireless communication device. The wireless communication device, in turn, must send the data to the backup server in response to that request.

Thus, the backup of data is driven by the wireless communication device and initiated by the user. Further, claim 1 required that the server will responsively request the wireless communication device for only the data that is not already earlier made available to the backup server from the wireless communication device or from other devices. The server, upon storing the backupdata for the wireless communication device, will also "provide, on request by the user, the data to the another computing device of the user." These recitations,

when properly viewed as a whole, as required by law, provides as novel, non-obvious, back up approach that optimally balance control, flexibility and efficiency between the user and the server.

Turning to the rejections, first, on page 2 of the Final Office Action, Dutta is cited as teaching in paragraph [0007] that "wireless device pushes request to client via proxy/gateway server." Applicants respectfully disagree. The cited paragraph does not teach or suggest that a wireless device pushes a request to a client. Instead, the cited paragraph discloses that a backup server initiates a backup process, and that the backup process may be initiated by pushing a request to the wireless client device. Thus, it is the backup server that pushes the request to the client. See also Figure 5 and paragraph [0043] (disclosing that data backup server 502 instructs the the proxy/gateway 504 to push a service loading content type (SL) to the wireless client 506 requesting that the client 506 send its data to the data backup server); paragraph [0031] (disclosing that at predetermined intervals or when notified that a user has powered on a wireless device, data backup server 170 pushes a command to the wireless device instructing the wireless device to upload data); and paragraph [0054]; "To begin, the data backup server determines that it is time to backup data from a client.").

Dutta also does not teach or suggest "facilitate login, ***by a user*** of the communication apparatus, to a ***user account at a remote backup server***, the user account being ***accessible from . . . another computing device*** of the user." Dutta does not teach or suggest a user account at a remote backup server, login to the account by the user, or that the user account is accessible from another computing device of the user. To the contrary, Dutta explicitly states that the backup server pushes a command to the wireless device to upload data, and then stores the information (paragraph [0031]). The information is stored with an indication of ownership and the owner may request to download saved data, for example, after losing information due to a battery failure. "**All of this is performed without notification of or action on the part of the user** . . . " (paragraph [0031]).

The remaining passages cited also fail to teach or suggest "login, by a user . . . to a user account at a remote backup server . . . ." In paragraphs 17-20, Dutta discloses that a firewall located at proxy server 106 precludes unwanted communications from entering LAN/WAN 104. This is not a "login, ***by a user*** . . . to ***a user account at a remote backup***

server . . . ." Applicants note that proxy server 106 couples computer 120 and phone 122, via LAN/WAN 104, to IP network 102. However, wireless handsets 132 and wirelessly enabled laptop computers are coupled to IP network 102 via cellular network 112 and gateway 114, neither of which are dislcosed as having a firewall configuration (see also e.g. Figure 1). These features do not teach or suggest the above recitation.

Next, the cited passage of Dutta does not teach or suggest "facilitate designation, by the user, of data on the wireless computing apparatus to be backed up by the backup server." Dutta discloses in the cited pasage that a data backup server isntructs the proxy/gateway 504 to push a SL to the wireless client requesting that the client send its data to the data backup server. Applicants find no teaching or suggestion in this passage, in Figure 4, or in the description of Figure 4 (paragraphs [0040]-[0042]) relevant to the selection of data to be backed up.

Dutta further fails to teach or suggest "generate a hash value . . ." and "communicate a request to the backup server to back up the designated data, including said hash value . . . ." Dutta does not disclose hash values. And as discussed above, Dutta teaches that the backup server sends the request to the client.

Dutta also does not address the association of the data with other user accounts, or provision of the data to another computing device of the user. Dutta merely discloses that if client 506 loses the backed up data, then *client 506* may retrieve the data from data backup server 502 and reload the data (paragraph [0046]). Thus, Dutta also does not teach or suggest "send said data to said backup server in response to said request from the backup server, ***wherein the backup server is configured to*** store the data, to ***associate the stored data with*** said user account as well as ***other user accounts*** subsequently wanting to backup the same data, ***and to provide, on request by the user, the data to the another computing device of the user***."

As conceded on page 4 of the Final Office Action, Dutta does not teach or suggest "only after said backup server determines that said data was not already earlier made available to said backup server from the wireless communication device or other devices, receive a request from said backup server to send said data to said backup server . . . ." or that

the identifier is a hash value. However, the Final Office Action asserts paragraph [0043] for teaching setting predefined conditions for backup. This passage merely discloses that the time at which a backup server initiates the backup process may be set at predetermined intervals or upon notification that the client has been powered on. Paragraph [0054] further states that *the data backup server* determines that it is time to backup data from a client. Thus, at most, the cited passage dislcoses that any "predefined" condition for backup is set by the backup server, not by the client or user.

Finally, when viewed properly as a whole, the cited figures and passages of Dutta teach a backup process *initiated and driven by a backup server*. This is contrary to the recitations of claim 1.

For at least the above reasons, Dutta fails to teach or suggest the above recitations of claim 1.

Andersen and Ramasubramani do not remedy the deficiencies of Dutta.

First, as conceded on page 5 of the Final Office Action, Dutta and Andersen do not disclose a login. Thus, these two references fail to teach or suggest "facilitate login, by a user of the wireless communication apparatus, to a user account at a remote backup server . . . ."

Like Dutta, Andersen does not teach or suggest "the user account being accessible from the wireless communication apparatus as well as from another computing device of the user" or "wherein the backup server is configured to . . . provide, on request by the user, the data to another computing device of the user." Instead, Andersen **teaches away** from these recitations by disclosing that the backup server maintains a collection of past catalogs that the backup client generated during previous backup sequences performed for that particular computing device (see e.g. col. 5, lines 43-47). The data portions to be restored are selected from the catalogs, and are provided to the computerized device in their original locations such that they contain their original file attributes (see e.g. col. 5, lines 51 to col. 6, line 12). Therefore, at most, the backup server of Andersen is configured to provide the data only to the same computing device that generated the catalog during a previous backup.

Ramasubramani was cited for teaching that a gateway is used compare access privileges of users through use of a password in which it is compared against registered user accounts to determine grant permissions. This was asserted in the Final Office Action as teaching, in combination with the disclosures of Dutta and Andersen, the "login" of claim 1.

Applicants respectfully disagree. The "user account" of Ramasubramani is a user account in proxy server 114, not "a user account at a remote backup server." The cited passages first refer to a request from the user of a mobile device 302 for certificates from user-specified Certification Authorities (CA's). The mobile device makes a request to connect to proxy server 114, the device ID is extracted from the request, and the user is prompted for a username and password. The cited passage then states that "username and password **are not the required information for the mobile device 302 to access the account 324**, rather the user is given a permission to administrate the username and password." Once a username and password are set, the user can go to any computer to manipulate the (proxy server) account 324. From PC 314, the user can manipulate the account 324 more efficiently; the user is prompted at the PC 314 to enter the username and password to get through the gateway 354. Once through the gateway, the user of the PC 314 can request a special certificate from a CA and place the certificate in the account for the mobile device 302 to use.

Thus, Ramasubramani does not teach or suggest a wireless communication device with executable instructions to "facilitate login, by a user of the wireless communication apparatus, to a user account at a remote backup server . . . ." On the contrary, Ramasubramani teaches that the user of the mobile device does not need to login to the proxy server account – the device ID is used to verify the account. And Ramasubramani does not disclose logging into an account at a backup server.

Finally, a person having ordinary skill in the art would lack motivation to combine the references as suggested. Dutta is directed to a backup method that is "performed without notification of or action of the part of the user." In addition, Andersen is directed to a backup method that requires backup data to be selected by a client device from among catalogs of previous backups of data from only that same device. Thus, adding a user login feature to either (or to both in combination) would be counterintuitive. A user login would decrease the

convenience of Dutta's invention, and would not be necessary in Andersen's invention. For at least these reasons, Applicants respectfully maintain that the suggested combination is improper.

For at least the above reasons, the combination of Dutta, Andersen and Ramasubramani fails to teach or even suggest the recitations of claim 1. Accordingly, claim 1, as amended, is allowable over Dutta, Andersen and Ramasubramani combined.

Claim 12 recites features substantially similar to those of claim 1. Accordingly, for at least the same reasons, claim 12 is also allowable over Dutta, Andersen, and Ramasubramani.

With respect to claims 11 and 16, Applicants note that U.S. Patent No. 6, 609, 138 to Merriam ("Merriam") does not remedy the above-discussed deficiencies of Dutta. For at least the reasons discussed above, Dutta does not teach or suggest at least the following recitations: "facilitate a user of the wireless communication apparatus in *logging into a user account of the user on a backup server*, using the wireless communication apparatus . . .", "wherein the backups performed for the wireless communication apparatus include backups taken from the wireless communication apparatus ***and backups taken from other devices***", "***determine whether the requested previous backups are not on the wireless communication device***, and ***whether the requested previous backups are compatible with the wireless communication apparatus***", and "***only on determining that the selected previous backups are currently not on the wireless communication apparatus and are compatible with the wireless communication apparatus, request the selected previous backups from the backup server***".

Merriam was cited for teaching "defining rules for backup." Merriam merely discloses a repository for hoding electronic messages according to a set of archive storage rules (see e.g. Abstract). Archive storage manager 318 and the client operate together to transfer a copy of a message to be archived from the post office 130 to the archive facility 140. The archive storage manager determines whether an archive token should be generated for, or removed from, a message based on the rules for archive storage 332 (col. 5, lines 1-10). The archive storage manager "determines which messages passing through a post office

facility are consistent with current rules for archive storage and will be directed to the archive repository 432 for later retrieval" (col. 6, lines 59-63).

Like Dutta, Merriam fails to teach or suggest the above features of claim 11. Therefore, claim 11 is allowable over Dutta and Merriam.

Claim 16 recites features substantially similar to those of claim 11, and is therefore also allowable over Dutta and Merriam for at least the same reasons.

Claims 2, 3, 5-10 and 13-15 depend from claims 1 and 12, incorporating their recitations. Thus, for at least the same reasons, claims 2, 3, 5-10, and 13-15 are allowable over Dutta, Andersen and Ramasubramani combined. These claims are further allowable over the cited combination by virtue of their additional recitations, which are not taught or suggested by the cited referencees.

CONCLUSION

In view of the foregoing, reconsideration and allowance of all pending claims is respectfully solicited. If the Examiner has any questions concerning the present paper, the Examiner is kindly requested to contact the undersigned at (206) 407-1513. If any fees are due in connection with filing this paper, the Commissioner is authorized to charge the Deposit Account of Schwabe, Williamson and Wyatt, P.C., No. 50-0393.

Respectfully submitted,
SCHWABE, WILLIAMSON & WYATT, P.C.

Date: May 27, 2010

by: /Jo Ann Schmidt/
Jo Ann Schmidt
Reg. No.: 62,255

Schwabe, Williamson & Wyatt, P.C.
Pacwest Center, Suites 1600-1900
1211 SW Fifth Avenue
Portland, Oregon 97222
Telephone: 503-222-9981